



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG

Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS)

Version vom Februar 2021

Inhaltsverzeichnis

1	Allgemeine Erläuterungen	3
1.1	Ausgangslage	3
1.2	Bezüge zu anderen Regulierungen	3
1.2.1	Kostenlose Tests	3
1.2.2	Erwerbsersatz im Quarantänefall.....	4
1.2.3	Covid-19-Verordnung Pilotversuch Proximity-Tracing.....	4
2	Internationale Interoperabilität	4
3	Erläuterung der einzelnen Bestimmungen	5
Artikel 1	Gegenstand	5
Artikel 2	Aufbau.....	5
Artikel 3	Freiwilligkeit	6
Artikel 4	Verantwortliches Bundesorgan.....	6
Artikel 5	Funktionsweise im Grundbetrieb	7
Artikel 6	Funktionsweise nach einer Infektion	8
Artikel 8	Inhalt des Codeverwaltungssystems	10
Artikel 8a	Art des Zugriffs auf das Codeverwaltungssystem	10
Artikel 9	Zugriff auf das Codeverwaltungssystem über das Frontend.....	10
Artikel 9a	Zugriff auf das Codeverwaltungssystem über die Schnittstelle	11
Artikel 10	Leistungen Dritter	11
Artikel 11	Protokoll über Zugriffe	12
Artikel 12	Bekanntgabe zu Statistikzwecken	12
Artikel 13	Vernichtung der Daten	13
Artikel 14	Überprüfung des Quellcodes	13
Artikel 15	Deaktivierung der SwissCovid-App und Berichterstattung	13
Artikel 15a	Verbindung des PT-Systems mit entsprechenden ausländischen Systemen	13
Artikel 16	Aufhebung eines anderen Erlasses	14
Artikel 16a	Nachführung des Anhangs	14
Artikel 17	Inkrafttreten und Geltungsdauer	15

1 Allgemeine Erläuterungen

1.1 Ausgangslage

Angesichts der aktuell hohen Fallzahlen sind das Unterbrechen der Infektionsketten durch Isolation von positiv getesteten Personen und die Verordnung einer Quarantäne für deren enge Kontakte im Rahmen des *Contact Tracing* durch die zuständigen kantonalen Behörden weiterhin wichtige Massnahmen zur Bewältigung der Covid-19-Pandemie in der Schweiz.

Ein Proximity-Tracing-System, also die SwissCovid-App inklusive der weiteren notwendigen Komponenten, kann das traditionelle *Contact Tracing* nicht ersetzen; es kann jedoch als unterstützendes Instrument eingesetzt werden. Dies gilt insbesondere, wenn es von Personen verwendet wird, die sehr mobil sind und sich wiederholt in Bereichen mit einem hohen Personenaufkommen und ihnen persönlich nicht bekannten Personen aufhalten.

Mit den beiden gleichlautenden Motionen SPK-NR 20.3144 vom 22. April 2020 und SPK-SR 20.3168 vom 30. April 2020 (Gesetzliche Grundlagen zur Einführung der Corona-Warn-App [Corona-Proximity-Tracing-App]) wurde der Bundesrat aufgefordert, die notwendige gesetzliche Grundlage zur Einführung von Corona-Warn Apps («Corona Proximity Tracing»-App) dem Parlament vorzulegen. Mit der Botschaft zu einer dringlichen Änderung des Epidemiengesetzes (EpG)¹ im Zusammenhang mit dem Coronavirus (Proximity-Tracing-System) vom 20. Mai 2020 (BBl 2020 4461) unterbreitete der Bundesrat dem Parlament einen solchen Regelungsvorschlag. Dieser beinhaltete in Erfüllung der beiden Motionen eine technische Lösung, welche keine personenbezogenen Daten zentral speichert, und eine freiwillige Verwendung der betreffenden App. Im Zuge der parlamentarischen Beratung haben National- und Ständerat den bundesrätlichen Vorschlag einerseits ergänzt, insbesondere um einen Anspruch auf kostenlose Tests auf Infektion und auf Antikörper gegen Nachweis der Benachrichtigung, dass man potenziell dem Coronavirus ausgesetzt war (siehe dazu Ziff. 1.2.1 nachfolgend). Andererseits hat das Parlament dem Bundesrat zudem empfohlen, parallel eine Lösung zu prüfen, wonach auch bei Personen, die durch das System benachrichtigt werden und sich freiwillig in Selbstquarantäne begeben, ein Anspruch auf Erwerbsersatz entsteht, sofern sie aus der Quarantäne die Erwerbsarbeit nicht fortsetzen können (siehe dazu Ziff. 1.2.2 nachfolgend). Die Vorlage wurde von beiden Räten der Schweizerischen Bundesversammlung für dringlich erklärt und in der Schlussabstimmung vom 19. Juni 2020 verabschiedet.

Seit dem 25. Mai 2020 fand zudem der Pilotversuch zum Schweizer PT-System statt. Die SwissCovid-App ersetzt die im Pilotversuch getestete App, wobei das System insgesamt weitergeführt wird.

1.2 Bezüge zu anderen Regulierungen

1.2.1 Kostenlose Tests

Eine Person, die durch das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 nach Artikel 60a EpG (PT-System) darüber benachrichtigt wurde, dass sie potenziell dem Coronavirus ausgesetzt war, kann gegen Nachweis der Benachrichtigung kostenlos Tests auf Infektion mit dem Coronavirus und auf Antikörper gegen das Coronavirus durchführen lassen (Art. 60a Abs. 4 EpG). Der Bundesrat hat dieses Recht auf kostenlose Tests und die Übernahme der Testkosten nicht in der vorliegenden Verordnung ausgeführt. Er regelt die Kriterien und das Verfahren zur Übernahme der Testkosten in den Artikeln 26 - 26c und Anhang 6 der Covid-19-Verordnung 3 vom 19. Juni 2020 (SR 818.101.24). Dabei ist das Recht auf einen kostenlosen Test nach einer Benachrichtigung durch die SwissCovid-App Teil der für die Kostenübernahme relevanten Verdachts-, Beprobungs- und Meldekriterien des BAG vom 27. Januar 2021².

¹ Epidemiengesetz vom 28. September 2012 (SR 818.101).

² Aktueller Stand jeweils abrufbar unter www.bag.admin.ch > Krankheiten > Infektionskrankheiten bekämpfen > Meldesysteme für Infektionskrankheiten > Meldepflichtige Infektionskrankheiten > Meldeformulare.

1.2.2 Erwerbsersatz im Quarantänefall

Mit Schreiben der SGK-NR und der SGK-SR wurde dem Bundesrat empfohlen, eine Lösung zu prüfen, wonach auch bei Personen, die durch das PT-System benachrichtigt werden und sich freiwillig in Selbst-quarantäne begeben, ein Anspruch auf Erwerbsersatz entsteht, sofern sie aus der Quarantäne die Erwerbsarbeit nicht fortsetzen können. Dabei ist jedoch wichtig zu betonen, dass allein die entsprechende Benachrichtigung zu keinem Anspruch auf Lohnfortzahlung oder Erwerbsersatzentschädigung führt. Vielmehr wird die «Infoline SwissCovid» (kostenlose Beratung, die im Auftrag des Bundesamtes für Gesundheit [BAG] als nationale Hotline betrieben wird) denjenigen von der App gewarnten Personen, welche nicht von zu Hause aus arbeiten können, raten, dass sie den zuständigen kantonalen Dienst kontaktieren. Dieser wird auf der Basis eines Gesprächs entscheiden, ob er eine Quarantäne gegenüber der betroffenen Person anordnen wird. Wird eine Quarantäne angeordnet bzw. verfügt, so hat die betroffene Person nach vorherrschender Meinung Anspruch auf Lohnfortzahlung (nach Art. 324 oder 324a OR). Diese Frage wurde aber bisher, soweit ersichtlich, gerichtlich noch nicht entschieden. Der Anspruch auf Erwerbsersatz wird in Artikel 15 des Covid-19-Gesetzes vom 25. September 2020 (SR 818.102) und in der Covid-19-Verordnung Erwerbsausfall vom 20. März 2020 (SR 830.31) geregelt.

1.2.3 Covid-19-Verordnung Pilotversuch Proximity-Tracing

Zwischen dem 25. Mai 2020 und dem 25. Juni 2020 wurde das Schweizer PT-System im Rahmen eines Pilotversuchs gestützt auf Artikel 17a des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) und die Covid-19-Verordnung Pilotversuch Proximity-Tracing vom 13. Mai 2020 (AS 2020 1589) getestet. Dieser Pilotversuch wurde mit Inkrafttreten der gesetzlichen Grundlage (Art. 60a EpG) und der vorliegenden Verordnung durch den ordentlichen Betrieb des PT-Systems abgelöst. Die Covid-19-Verordnung Pilotversuch Proximity-Tracing wird mit Artikel 16 der vorliegenden Verordnung aufgehoben.

2 Internationale Interoperabilität

Ein wichtiges Ziel des PT-Systems ist die Kompatibilität der SwissCovid-App mit gleichartigen ausländischen Apps. Bisher kann die SwissCovid-App die teilnehmenden Personen jedoch nicht benachrichtigen, wenn sie eine epidemiologisch relevante Annäherung zu infizierten Nutzerinnen oder Nutzern einer gleichartigen ausländischen App gehabt haben (z.B. zu Grenzgängern und Touristen im Inland oder Kontakten im Ausland). Umgekehrt können Nutzerinnen und Nutzer einer gleichartigen ausländischen App nicht gewarnt werden, wenn sie eine epidemiologisch relevante Annäherung zur SwissCovid-App hatten. Ebenso ist es auf einem Mobiltelefon aber auch nicht möglich, gleichzeitig mehrere nationale Covid-Apps zu betreiben, welche das Exposure Notification Framework von Apple und Google nutzen (siehe dazu Erläuterung zu Art. 5 Abs. 2 und 3). Die Verbindung des PT-Systems mit entsprechenden ausländischen Systemen (internationale Interoperabilität) ist daher ein bedeutendes Anliegen, um die Infektionsketten auch im Inland besser unterbrechen zu können, indem etwa Grenzgänger und Touristen mit ausländischen Apps ebenfalls über eine Infektion benachrichtigen und benachrichtigt werden können. Das Gesetz gibt zur internationalen Interoperabilität der SwissCovid-App vor, dass ein grenzüberschreitender Austausch nur in Frage kommt, wenn ein mit der Schweiz vergleichbares Datenschutzniveau gewährleistet ist (Art. 62a EpG). Weiter müssen auch die Grundprinzipien des PT-Systems berücksichtigt werden. Artikel 15a konkretisiert nun die Voraussetzungen, unter denen das schweizerische PT-System mit entsprechenden ausländischen Systemen verbunden werden kann. Das Ziel ist es, dass damit nicht nur die rechtlichen Grundlagen für eine Verbindung in einem ersten Schritt konkret mit Deutschland geschaffen werden, sondern dass auf dieser Grundlage das PT-System zukünftig auch mit weiteren ausländischen Systemen verbunden werden kann, sofern die Voraussetzungen von Artikel 62a EpG und Artikel 15a VPTS erfüllt sind.

Dabei stellt sich im Hinblick auf eine wirksame Pandemiebekämpfung die Grundfrage, ob infizierten Nutzerinnen und Nutzern wählen können, mit welchen verbundenen in- und ausländischen Systemen sie ihre Schlüssel teilen wollen (d.h. welche Apps sie deren Nutzerinnen und Nutzer benachrichtigen lassen wollen). Für eine Lösung, die eine selektive Wahlfreiheit ermöglicht, sprechen insbesondere die

informationelle Selbstbestimmung der betroffenen Personen sowie strategische Überlegungen. Die informationelle Selbstbestimmung gebietet, den Individuen grösstmögliche Entscheidungsfreiheit über das Schicksal ihrer persönlichen Daten zu belassen. Aus strategischer Sicht wiederum könnte die Nichtgewährung einer solchen Wahlfreiheit zu einer verminderten Akzeptanz in der Bevölkerung führen. Damit besteht auch ein gewisses Risiko einer Beeinträchtigung der Wirksamkeit des inländischen PT-Systems, wenn eine teilnehmende Personen entweder nur alle verbundenen Systeme oder niemanden benachrichtigen kann. Demgegenüber sprechen für die Lösung des sog. «One World»-Prinzips (Einwilligung zur einheitlichen Benachrichtigung in allen verbundenen Systemen) zunächst Effektivitätsüberlegungen (kein «Rosinenpicken»). Nutzerinnen und Nutzer sollen über mögliche Infektionen gewarnt werden, auch wenn sie im Ausland geschahen. Wie erwähnt sollen Nutzerinnen und Nutzer einer inländischen App auch gewarnt werden, falls sich infizierte Nutzerinnen und Nutzer einer ausländischen App im Inland befunden haben, und umgekehrt. Im Sinne der internationalen Interoperabilität als bestmögliche Meldung von exponierten Personen bedeutet das für die nationalen Systeme: Es sollten einheitlich auch die privaten Schlüssel infizierter Nutzerinnen und Nutzer von ausländischen Systemen (Grenzgänger, Touristen, Gäste etc.) zur Warnung der inländischen Bevölkerung enthalten sein; umgekehrt sollte auch die Übertragung aller privaten Schlüssel von infizierten Nutzerinnen und Nutzern der SwissCovid App in die verbundenen ausländischen Systeme erfolgen. Nicht zuletzt gilt es zu beachten, dass sich auch die EU-Staaten – inklusive Norwegen – gemeinsam auf die Umsetzung des One World-Ansatzes verständigt haben. Aus diesen Gründen folgt auch die Schweiz dem «One World»-Prinzip. Die Benutzeroberfläche und die datenschutzrechtlichen Dokumentationen der SwissCovid-App werden dahingehend angepasst, dass die teilnehmenden Personen informiert werden und einwilligen müssen, dass eine allfällige Bekanntgabe ihrer Schlüssel auch an ausländische Systeme bzw. an deren Nutzer erfolgt.

3 Erläuterung der einzelnen Bestimmungen

Artikel 1 Gegenstand

Gegenstand dieser Verordnung bilden die Einzelheiten der Organisation, des Betriebs und der Datenbearbeitung des PT-Systems. Der Bundesrat erfüllt damit seinen Auftrag, diese Einzelheiten auf Verordnungsstufe zu regeln (Art. 60a Abs. 7 EpG).

Artikel 2 Aufbau

Das PT-System basiert technisch auf dem sogenannten DP-3T-Konzept (*Decentralized Privacy Preserving Proximity Tracing*), welches unter anderem von der Eidgenössischen Technischen Hochschule Lausanne entwickelt wurde, und damit auf dem Grundsatz des Datenschutzes durch Technikgestaltung («*privacy by design*»). Es ist mit innovativen kryptografischen Methoden und einer dezentralisierten Datenbearbeitung darauf ausgerichtet, dass möglichst keine Angaben zu bestimmten oder bestimmbar Personen (Personendaten) vorhanden sind. Demnach sind alle Komponenten des PT-Systems sowie dessen Betrieb so ausgestaltet, dass personenbezogene Daten nur dann bearbeitet werden, wenn dies systembedingt erforderlich ist. Entsprechend sind bei der Datenbearbeitung alle angemessenen technischen und organisatorischen Massnahmen zu treffen, um zu verhindern, dass die teilnehmenden Personen bestimmbar sind (Art. 60a Abs. 5 Bst. a EpG). Zugleich sieht das PT-System vor, dass die Daten so weit wie möglich auf dezentralen Komponenten, d.h. auf den Mobiltelefonen der teilnehmenden Personen, bearbeitet werden. Insbesondere dürfen Daten, die auf dem Mobiltelefon einer teilnehmenden Person über andere Personen erfasst werden, ausschliesslich auf diesem Mobiltelefon bearbeitet und gespeichert werden (Art. 60a Abs. 5 Bst. b EpG). Der Aufbau des PT-Systems gemäss Artikel 2 stellt sicher, dass diesen Anforderungen nachgekommen wird.

Nach Absatz 1 gliedert sich das PT-System in mehrere Komponenten, in welchen jeweils nur diejenigen Daten gespeichert werden, die zum Betrieb des Gesamtsystems erforderlich sind. Es umfasst einerseits ein System zur Verwaltung der Annäherungsdaten (VA-System), das aus einer App-Software für das Mobiltelefon (SwissCovid-App) und einem entsprechenden Backend besteht (VA-Backend). Das PT-System umfasst andererseits ein System zur Verwaltung von Codes zur Freischaltung der Benachrich-

tigungen (Codeverwaltungssystem), das aus einem webbasierten Frontend und einem Backend besteht. Der Inhalt, die Funktionsweise und das Zusammenspiel der verschiedenen Komponenten wird detailliert bei den Artikeln 5, 6 und 9 geregelt (siehe entsprechende Erläuterungen).

Absatz 2 hält fest, dass das VA-Backend und das Codeverwaltungssystem als zentrale Server vom BAG betrieben werden. Diese, für das Funktionieren der SwissCovid-App erforderlichen zentralen Bestandteile, werden im Auftrag des BAG vom Bundesamt für Informatik und Telekommunikation (BIT) entwickelt und betrieben. Die Verwendung erforderlicher zentraler Bestandteile ändert nichts daran, dass jegliche auf dem Mobiltelefon einer teilnehmenden Person über andere Personen erfassten Daten ausschliesslich auf diesem Mobiltelefon bearbeitet und gespeichert werden (Art. 60a Abs. 5 Bst. b EpG).

Zu beachten gilt, dass das Verbindungssystem nach Artikel 15a VPTS als solches nicht Komponente des PT-Systems nach Artikel 60a EpG ist. Insofern greifen dafür etwa die Pflicht zum Betrieb durch das BAG (Art. 60a Abs. 1 Satz 1 EpG) oder die Grundsätze nach Artikel 60a Absatz 5 EpG nicht. Vielmehr handelt es sich beim Verbindungssystem um ein zusätzliches System, um das PT-System mit entsprechenden ausländischen Systemen zu verbinden gemäss Artikel 62a EpG. Die dafür geltenden Regeln konkretisiert Artikel 15a VPTS (siehe entsprechende Erläuterungen).

Artikel 3 Freiwilligkeit

Absatz 1 präzisiert die gesetzliche Vorgabe der freiwilligen Teilnahme am PT-System (Art. 60a Abs. 3 Satz 1 EpG) dahingehend, dass sowohl die Installation als auch der Einsatz (d.h. insbesondere die Aktivierung der Bluetooth-Funktion) der SwissCovid-App freiwillig sind.

Ergänzend anzumerken bleibt, dass von Gesetzes wegen Behörden, Unternehmen und Einzelpersonen keine Person aufgrund ihrer Teilnahme oder Nichtteilnahme am PT-System bevorzugen oder benachteiligen dürfen und abweichende Vereinbarungen unwirksam sind (Art. 60a Abs. 3 Satz 2 EpG).

Absatz 2 stellt darüber hinaus klar, dass im Infektionsfall die Eingabe des Freischaltcodes zur Benachrichtigung der übrigen teilnehmenden Personen, dass diese potenziell dem Coronavirus ausgesetzt waren, ebenfalls freiwillig ist und eine ausdrückliche Einwilligung der infizierten Person voraussetzt. Aufgrund des «One-World»-Prinzips erfolgt nach einer ausdrücklichen Einwilligung nicht nur die Benachrichtigung von teilnehmenden Personen am inländischen PT-System, sondern auch von Nutzerinnen und Nutzern verbundener ausländischer Systeme (siehe Internationale Interoperabilität, Ziff. 2 vorstehend). Die Benachrichtigung der potenziell dem Coronavirus ausgesetzten Personen erfolgt zwar ohne Angabe von Personendaten; trotzdem kann eine benachrichtigte Person unter Umständen anhand der Sozialkontakte der letzten Tage eruieren, um wen es sich bei der infizierten Person handelt, zu welcher sie in epidemiologisch relevanten Kontakt war. Da damit der benachrichtigten Person auch bewusst wird, dass sich die betreffende Person mit dem Coronavirus infiziert hat, handelt es sich um die Bekanntgabe von besonders schützenswerten Personendaten, welche eine ausdrückliche Einwilligung der betreffenden Person voraussetzt (vgl. Art. 3 Bst. c Ziff. 2 und Art. 4 Abs. 5 Satz 2 DSG). Die App informiert die infizierte Person über diesen Fakt. Erst mit der Bestätigung in der SwissCovid-App, dass die infizierte Person dies verstanden hat und trotzdem die anderen teilnehmenden Personen benachrichtigen möchte, werden die anderen Personen benachrichtigt.

Artikel 4 Verantwortliches Bundesorgan

Auf das PT-System ist die Bundesgesetzgebung über den Datenschutz anwendbar (Art. 60a Abs. 6 EpG). Das Gesamtsystem mit allen Komponenten (einschliesslich der SwissCovid-App) untersteht integral der datenschutzrechtlichen Verantwortung des systembetreibenden BAG. So werden das VA-Backend und das Codeverwaltungssystem im Auftrag des BAG zwar vom BIT betrieben (siehe Erläuterung zu Art. 2 Abs. 2). Dies ändert aber nichts daran, dass die datenschutzrechtlichen Ansprüche (insb. auf Auskunft und Berichtigung; vgl. Art 5 Abs. 2 und Art. 8 DSG) gegebenenfalls gegenüber dem BAG geltend zu machen sind. Diese Ansprüche greifen allerdings nur, soweit tatsächlich Personendaten (Art. 3 Bst. a DSG) vorhanden sind und das BAG auf diese auch Zugriff hat. Das wird weitest möglich gerade verhindert durch die massgeblichen Grundsätze des Datenschutzes durch Technikgestaltung (insb. Art. 60a Abs. 5 Bst. a und b EpG; siehe dazu Erläuterungen zu Artikel 2). So ist es dem BAG beispielsweise nicht möglich, Auskunft über die zu einer bestimmten Person erfassten Annäherungen zu

erteilen oder diese Daten zu korrigieren. Das BAG kann solche Daten nicht einsehen, da sie dezentral einzig auf den Mobiltelefonen gespeichert werden.

Artikel 5 Funktionsweise im Grundbetrieb

Absatz 1 beschreibt den Inhalt der im VA-Backend gespeicherten Daten, welche es den SwissCovid-Apps zum Abruf zur Verfügung stellt. Es handelt sich um alle privaten Schlüssel (sog. «private keys») von nachweislich infizierten teilnehmenden Personen in dem Zeitraum, in welchem epidemiologisch eine grosse Wahrscheinlichkeit besteht, dass die infizierte Person bereits ansteckend war (siehe insb. Erläuterungen zu Art. 6 Abs. 3). Zusätzlich enthält das VA-Backend auch das jeweilige Datum des Schlüssels.

Absätze 2 und 3: *Absatz 2* legt die Funktionen fest, welche die SwissCovid-App gemäss *Einleitungssatz* «unter Verwendung einer Schnittstelle zum Betriebssystem des Mobiltelefons» erfüllt. Konkret ist die betreffende Schnittstelle nutzbar im gemeinsam von Google und Apple entwickelten sogenannten «*Exposure Notification Framework*». Sie steht zur Verfügung mit den aktuellsten iOS- und Android-Versionen von Apple bzw. Google (ab Version 13.5 für iOS bzw. Version 6 und höher mit den neuesten Google Play Diensten für Android). Die darauf abgestützte SwissCovid-App ist daher grundsätzlich funktionsfähig auf Betriebssystem-Versionen, welche die betreffende Schnittstelle beinhalten. Durch die Verwendung der Schnittstelle ist insbesondere die Bluetooth-Messung genauer und der zusätzliche Stromverbrauch wird auf ein Minimum reduziert. Ausserdem ermöglicht die Schnittstelle, dass die App im Hintergrund läuft, falls sie aktiviert ist. Aus technischer Sicht unterstützt das zugrundeliegende Betriebssystem respektive die betreffende Schnittstelle zum Betriebssystem des Mobiltelefons die SwissCovid-App massgeblich bei der Erfüllung ihrer Funktionen, auch wenn Betriebssystem bzw. Schnittstelle nicht eigentlicher Bestandteil der SwissCovid-App (und insofern auch keine Komponenten des PT-Systems nach Artikel 2) sind.

Aus rechtlicher Sicht sind für das PT-System mit seinen Komponenten wiederum die Vorgaben nach Artikel 60a EpG und dieser Verordnung massgeblich. Diese Vorgaben erfassen als solche die von der SwissCovid-App verwendeten Funktionen der Betriebssysteme von Google und Apple nicht. Vor diesem Hintergrund rechnet die Verordnung die vom Betriebssystem erbrachten massgeblichen Funktionen rechtlich der SwissCovid-App zu. Konkret bedeutet das insbesondere:

- *Absatz 3* hält fest, dass *die über die Schnittstelle genutzten Funktionen der Betriebssysteme* die Vorgaben von Artikel 60a EpG und dieser Verordnung erfüllen müssen, obwohl die Betriebssysteme von Google und Apple als solche nicht der vorliegenden Verordnung unterstehen. Dies bedeutet, dass bei einer Änderung der Android- oder iOS-Software im für die App relevanten Bereich, womit die Bestimmungen der Verordnung nicht mehr erfüllt wären, der Bundesrat entweder die Verordnung im Rahmen der gesetzlichen Vorgaben anpassen oder – falls dies nicht möglich ist – die Zusammenarbeit (Verwendung der Schnittstelle zum Betriebssystem) beenden müsste.
- Dabei ist nach *Absatz 3* das systembetreibende BAG verpflichtet, sich zu vergewissern, dass die über die Schnittstelle genutzten Funktionen der Betriebssysteme die entsprechenden Vorgaben einhalten, insbesondere indem es entsprechende Zusicherungen von Google und Apple einholt.
- Diesbezüglich anzumerken bleibt, dass Artikel 60a Absatz 5 Buchstabe e EpG für alle Komponenten des PT-Systems die Öffentlichkeit des Quellcodes und der technischen Spezifikationen statuiert, während Apple und Google als kommerzielle Unternehmen die Quellcodes für ihre Betriebssysteme (und die verwendete Schnittstelle) aber nicht offenlegen. Dieses Umstandes war sich der Gesetzgeber bei der Verabschiedung der betreffenden Bestimmungen bewusst. Absatz 3 hält daher klärend auch fest, dass die über die Schnittstelle genutzten Funktionen der Betriebssysteme die Regelung betreffend den Quellcode nach Artikel 60a Absatz 5 Buchstabe e EpG nicht erfüllen müssen. Das berührt hingegen die Publikation der technischen Spezifikationen (und die damit einhergehenden Verpflichtungen des BAG) nicht.

Im Detail funktioniert die SwissCovid-App zusammen mit dem Betriebssystem folgendermassen:

- *Buchstabe a:* Das Betriebssystem generiert jeden Tag einen neuen privaten Schlüssel, der keine Rückschlüsse auf die SwissCovid-App, das Mobiltelefon und die teilnehmende Person ermöglicht.

- **Buchstabe b:** Die Erfassung der Annäherungen zwischen teilnehmenden Personen basiert auf der Bluetooth-Funktechnologie; vom PT-System werden keine Standortdaten beschafft oder in anderer Art und Weise bearbeitet (Art. 60a Abs. 5 Bst. c EpG). So muss bei Geräten mit Android-Betriebssystemen zwar die Standortermittlung aktiviert sein, damit Bluetooth funktioniert. Die SwissCovid-App hat jedoch zu keiner Zeit Zugriff auf den Standort der teilnehmenden Personen. Innerhalb der Reichweite von Bluetooth tauscht sodann das jeweilige Betriebssystem mit allen anderen Betriebssystemen, welche ebenfalls eine von Google oder Apple autorisierte und kompatible App installiert haben, einen mindestens halbstündlich wechselnden Identifizierungscode (sog. «random ID») aus. Dieser wird aus einem aktuellen privaten Schlüssel gemäss Buchstabe a abgeleitet, kann aber nicht auf diesen Schlüssel zurückgeführt werden und ermöglicht ebenfalls keine Rückschlüsse auf die SwissCovid-App, das Mobiltelefon und deren Benutzerinnen und Benutzer.
- **Buchstabe c:** Das Betriebssystem speichert auf dem Mobiltelefon die empfangenen Identifizierungs-codes, die Signalstärke, das Datum und die geschätzte Dauer der Annäherung. Der Austausch funktioniert wie ausgeführt innerhalb der Reichweite der Bluetooth-Funktechnik. Mit anderen Worten werden alle Identifizierungs-codes innerhalb von potenziell bis zu 50 Metern ausgetauscht und gespeichert. Dabei ist der Austausch und die Speicherung nicht auf Mobiltelefone mit Schweizer SwissCovid-Apps beschränkt; beides ist grundsätzlich möglich für alle Mobiltelefone, welche das «*Exposure Notification Framework*» für ihre (untereinander kompatiblen) Proximity-Tracing-Apps verwenden. Dies ist aus technischer sowie datenschutzrechtlicher Sicht aus folgenden Gründen erforderlich: Technisch gesehen werden je nach Mobilfontyp unterschiedlich starke Bluetooth-Signalstärken verwendet. Die Verschlüsselung der ausgestrahlten Datenpakete umfasst auch die Angabe, wie stark das Sendemodul dieses Telefons gesendet hat, was zur Abschätzung der Distanz (anhand der empfangenen Signalstärke) durch das empfangende Mobiltelefon erforderlich ist. Ebenfalls kann das Betriebssystem anhand des ausgesendeten Identifizierungs-codes nicht erkennen, ob die schweizerische oder eine kompatible ausländische Proximity-Tracing-App verwendet wird. Zum datenschutzrechtlichen Schutz der teilnehmenden Personen wird eine Entschlüsselung u.a. der eingebetteten Signalstärke (und folglich von der SwissCovid-App daraus abgeleitet die Bestimmung der als epidemiologisch relevanten definierten Annäherungen gemäss Bst. e) erst *nach* einer Infektionsmeldung (im Hinblick auf eine Benachrichtigung) vorgenommen. Der Identifizierungscode kann mit anderen Worten nicht ohne den privaten Schlüssel der infizierten Person entschlüsselt werden. Das bedeutet: Nur wenn das PT-System gemäss Artikel 62a EpG mit einem entsprechenden ausländischen System verbunden wurde (d.h. angemessener Schutz der Persönlichkeit vorausgesetzt), kann es gegebenenfalls Identifizierungs-codes von Personen, welche ausländische Apps verwenden, ebenfalls entschlüsseln (und vice versa).
- **Buchstabe d:** Die SwissCovid-App ruft weiter periodisch eine Liste der privaten Schlüssel der infizierten Benutzerinnen und Benutzer ab und lässt vom Betriebssystem überprüfen, ob mindestens ein lokal gespeicherter Identifizierungscode mit einem privaten Schlüssel der Liste generiert wurde.
- **Buchstabe e:** Ist dies der Fall und sind die als epidemiologisch relevant definierten Annäherungsbedingungen erfüllt, so gibt die SwissCovid-App die Benachrichtigung aus. Aktuell sind gemäss *Ziffer 1 des Anhangs* diese epidemiologischen Annäherungsbedingungen erfüllt, wenn zu mindestens einem Mobiltelefon einer infizierten teilnehmenden Person eine räumliche Annäherung von 1,5 Metern oder weniger bestand (geschätzt anhand der Stärke der empfangenen Signale) und die Summe der Dauer aller solchen Annäherungen innerhalb eines Tages fünfzehn Minuten erreicht.

Artikel 6 Funktionsweise nach einer Infektion

Absatz 1 schreibt vor, dass im Falle einer (durch einen positiven Test auf SARS-CoV-2) nachgewiesenen Infektion eine berechnete Stelle (siehe dazu Erläuterungen zu Artikel 9 und 9a) mit der Einwilligung der infizierten Person einen einmalig einlösbaren und 24 Stunden gültigen (vgl. Art. 13 Abs. 2) Freischaltcode anfordern kann (sog. «Covidcode»). Dabei gibt sie im System das Datum des Auftretens der ersten Symptome, oder, falls die infizierte Person keine Symptome zeigt, das Testdatum ein.

Nach **Absatz 2** gibt die berechnete Stelle den Freischaltcode der infizierten Person bekannt. Diese kann den Freischaltcode innerhalb einer Bedenkfrist von 24 Stunden (Gültigkeitsdauer des Freischaltcodes) in ihre SwissCovid-App eingeben und bestätigen, dass sie die betreffenden teilnehmenden Personen benachrichtigen lassen will. Die Eingabe des Freischaltcodes und die Benachrichtigung der anderen

teilnehmenden Personen erfolgt damit nur mit der ausdrücklichen Einwilligung der infizierten Person (Art. 3 Abs. 2). Insbesondere nicht Gegenstand der Regelung ist die Art und Weise der Übermittlung der Freischaltcodes an die infizierte Person; dort ist die jeweils zuständige Stelle nach dem (Datenschutz-)Recht, das auf sie anwendbar ist, verantwortlich.

Nach *Absatz 3* bestätigt das Backend des Codeverwaltungssystems gegenüber der SwissCovid-App die Gültigkeit des eingegebenen Freischaltcodes. Vom Datum des Auftretens der ersten Symptome respektive des positiven Tests zieht es die Anzahl Tage gemäss Ziffer 2 des Anhangs ab und übermittelt dieses neue Datum der SwissCovid-App. Diese Anzahl Tage vor Auftreten der Symptome entspricht dem Zeitraum, in welchem epidemiologisch eine grosse Wahrscheinlichkeit vorliegt, dass die infizierte Person bereits ansteckend war, obwohl sie noch keine Symptome hatte (Beginn des epidemiologisch relevanten Zeitraums). Damit können auch Personen gewarnt werden, welche mit der infizierten Person in Kontakt waren, bevor diese selbst von ihrer Infizierung wusste, mitunter aber bereits ansteckend war. Gegenwärtig ist die Anzahl abzuziehender Tage gemäss bisherigen Erkenntnissen auf zwei festgelegt (siehe Anhang Ziffer 2). Da die Wissenschaft aber nach wie vor darüber diskutiert, ob der für die Ansteckung relevante Zeitraum bei einer Erkrankung mit dem Coronavirus eventuell auch länger als zwei Tage vor Symptombeginn beginnen könnte, erhält das Eidgenössische Departement des Innern (EDI) die Aufgabe, die Anzahl abzuziehender Tage entsprechend dem aktuellen Stand der Wissenschaften nachzuführen (siehe Art. 16a).

Nach *Absatz 4* sendet die SwissCovid-App nach Bestätigung der Gültigkeit des Freischaltcodes die folgenden Daten an das VA-Backend: alle privaten Schlüssel für jeden Tag ab dem Zeitpunkt, an dem eine Ansteckung wie beschrieben möglich war, sowie das Datum des jeweiligen Schlüssels.

Nach *Absatz 5* setzt das VA-Backend diese privaten Schlüssel mit ihrem jeweiligen Datum auf seine Liste zum Abruf durch die anderen SwissCovid-Apps, welche anhand der privaten Schlüssel auf dieser Liste vom Betriebssystem überprüfen lassen, ob sie zur infizierten Person in einem nahen Kontakt waren.

Nach *Absatz 6* erzeugt die SwissCovid-App nach der Übermittlung der privaten Schlüssel einen neuen privaten Schlüssel, von welchem nicht auf frühere private Schlüssel zurückgeschlossen werden kann. Momentan werden alle privaten Schlüssel so generiert, dass von ihnen nicht auf frühere private Schlüssel zurückgeschlossen werden kann, weshalb die App einfach regulär am nächsten Tag einen neuen privaten Schlüssel generiert. Absatz 6 bleibt jedoch insofern notwendig, als dass sie den Grundsatz festlegt, dass von den privaten Schlüsseln vor einer Meldung der Infizierung (welche im VA-Backend gespeichert werden) nicht auf die privaten Schlüssel nach einer gemeldeten Infizierung geschlossen werden darf. Dies um zu verhindern, dass beispielsweise eine Isolation der betreffenden Person mittels dieser privaten Schlüssel überwacht werden könnte (vgl. auch Art. 60a Abs. 2 Satz 2 EpG).

Artikel 7 Inhalt der Benachrichtigung

Absatz 1 gibt den Inhalt der Benachrichtigung vor, welche die teilnehmenden Personen gegebenenfalls gemäss Artikel 5 Absatz 2 Buchstabe e erhalten. Eine benachrichtigte Person wird von der SwissCovid-App informiert, dass sie potenziell dem Coronavirus ausgesetzt war (*Bst. a*) und an welchen Tagen dies der Fall war (*Bst. b*). Sie erfährt demgegenüber nicht, wer infiziert ist und die Benachrichtigung ausgelöst hat. Einzig der behandelnde Arzt oder die behandelnde Ärztin und die zugriffsberechtigte Fachperson gemäss Artikel 9 kennen die Identität der infizierten Person, welche den Freischaltcode eingibt. Es kann jedoch sein, dass die benachrichtigte Person anhand der Sozialkontakte der letzten Tage eruiert, um wen es sich bei der infizierten Person handeln kann. Dies lässt sich aber nicht verhindern und ist auch bei der traditionellen Nachverfolgung von Kontakten (klassisches *Contact Tracing*) nicht anders. Im Weiteren beinhaltet die Benachrichtigung den Hinweis auf die Infoline SwissCovid des BAG zur kostenlosen Beratung (*Bst. c*) sowie Verhaltensempfehlungen des BAG, die gemäss den jeweils aktuellen epidemiologischen Erkenntnissen auf eine Unterbrechung der Infektionsketten hinzuwirken versuchen (*Bst. d*).

Absatz 2 statuiert, dass das PT-System den teilnehmenden Personen keine Anweisungen erteilt. Das PT-System kann weder eine medizinische Einschätzung vornehmen, noch anstelle der zuständigen Behörden epidemienrechtliche Massnahmen anordnen (wie z.B. eine Quarantäne). Das PT-System und

die mit ihm bearbeiteten Daten dürfen von den zuständigen kantonalen Behörden auch nicht zur Anordnung und Durchsetzung von Massnahmen nach den Artikeln 33–38 EpG verwendet werden (Art. 60a Abs. 2 Satz 2 EpG). Insbesondere kann damit auch keine angeordnete Quarantäne überwacht werden. Das PT-System und die mit ihm bearbeiteten Daten dienen (rudimentäre statistische Auswertungen vorbehalten) letztlich «nur» der Benachrichtigung von Personen, die potenziell dem Coronavirus ausgesetzt waren (Art. 60a Abs. 2 Satz 1 EpG).

Artikel 8 Inhalt des Codeverwaltungssystems

Nach *Absatz 1* werden im Codeverwaltungssystem die folgenden Daten gespeichert: die Freischaltcodes (*Bst. a*); das Datum, an dem die ersten Symptome aufgetreten sind, oder, falls die infizierte Person keine Symptome hat, das Testdatum (*Bst. b*); schliesslich auch der Zeitpunkt der Vernichtung dieser Daten, die gemäss Artikel 13 Absatz 2 24 Stunden nach der Generierung des Codes erfolgt (*Bst. c*).

Absatz 2 hält fest, dass diese Daten keine Rückschlüsse auf die teilnehmenden Personen zulassen. Einzig die zugriffsberechtigte Person nach Artikel 9 weiss, für wen sie den Freischaltcode generiert. Diese Information wird jedoch nirgends im PT-System erfasst. Gegenüber der SwissCovid-App wird vom Codeverwaltungssystem die Gültigkeit des Freischaltcodes lediglich bestätigt; das Codeverwaltungssystem hat in keinem Moment die Information, welcher Person dieser Freischaltcode zugerechnet wird.

Artikel 8a Art des Zugriffs auf das Codeverwaltungssystem

Der Zugriff auf das Codeverwaltungssystem zur Anforderung des Freischaltcodes kann auf zwei unterschiedliche Arten erfolgen. Nach *Buchstabe a* kann eine Fachperson der berechtigten Stelle über das webbasierte Frontend auf das Codeverwaltungssystem zugreifen (siehe dazu Art. 9). Damit sich nicht zur Anforderung jedes einzelnen Freischaltcodes eine Fachperson im Codeverwaltungssystem einloggen sowie den Freischaltcode dann in einem zweiten Schritt der infizierten Person mittels Telefon, SMS oder E-Mail bekanntgeben muss, kann nach *Buchstabe b* der Zugriff auch über eine Schnittstelle zwischen dem Codeverwaltungssystem und einem System der berechtigten Stelle erfolgen (siehe dazu Art. 9a). Das ermöglicht etwa, dass in einem Arbeitsschritt (und mitunter automatisiert) den infizierten Personen mit dem positiven Testresultat zugleich auch der Freischaltcode bekanntgegeben werden kann.

Artikel 9 Zugriff auf das Codeverwaltungssystem über das Frontend

Absatz 1 definiert die zugriffsberechtigten Personen, die – für die jeweilige berechnete Stelle handelnd – den Freischaltcode mittels Zugriff auf das Frontend des Codeverwaltungssystems anfordern können.

- *Buchstaben a–d*: Der Freischaltcode kann zunächst durch diejenigen Personen generiert und herausgegeben werden, welche vom Kanton oder bei Militärangehörigem im Dienst vom Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) mit dem klassischen *Contact Tracing* betraut sind. Dabei kann der Kanton oder das VBS seine eigene Organisationsstruktur dazu verwenden, oder private Organisationen mit dem klassischen Contact Tracing beauftragen.
- *Buchstabe e*: Zugriffsberechtigt sind weiter auch Mitarbeiterinnen und Mitarbeiter von Arztpraxen (behandelnde Ärztin oder der behandelnde Arzt und deren Hilfspersonen).
- *Buchstabe f*: Die nach Artikel 16 EpG bewilligten Laboratorien führen u.a. molekularbiologische Analysen auf Sars-CoV-2 und immunologische Analysen auf Sars-CoV-2-Antigene durch und werten das Testergebnis aus. Sie sollen im Falle eines positiven Testergebnisses mit der Bekanntgabe des Resultats an die infizierte Person auch den Freischaltcode ausgeben können, damit die infizierten Personen so schnell wie möglich ihre betroffenen Kontaktpersonen informieren können, dass diese potenziell dem Coronavirus ausgesetzt waren.
- *Buchstabe g*: Aus den gleichen Überlegungen können auch Mitarbeiterinnen und Mitarbeiter von Einrichtungen nach Artikel 24 Absatz 1 Buchstabe b Covid-19-Verordnung 3, die immunologische Analysen auf Sars-CoV-2-Antigene mittels Schnelltests durchführen können (d.h. Arztpraxen, Apotheken und Spitäler sowie Testzentren, die vom Kanton oder in dessen Auftrag betrieben werden), den Freischaltcode ausgeben.

- *Buchstabe h:* In Zeiten hoher Fallzahlen und ausserordentlicher Belastung können die zugriffsberechtigten Fachpersonen den Freischaltcode mitunter nicht in einem sinnvoll kurzen Zeitraum ausgeben. Daher können auf Anfrage der infizierten Personen hin schliesslich auch Mitarbeiterinnen und Mitarbeiter der Infoline nach Artikel 7 Absatz 1 Buchstabe c den Freischaltcode ausgeben. Für solche Anfragen richtet das BAG im Rahmen der Infoline zur kostenlosen Beratung eine eigene Telefonnummer ein und gibt diese in der SwissCovid-App bekannt. Um sicherzustellen, dass tatsächlich lediglich nachweislich positiv getestete Personen einen Freischaltcode erhalten, erhalten die betreffenden Mitarbeiterinnen und Mitarbeiter der Infoline Zugriff auf das System «Meldungen» des Informationssystems nach Artikel 60 EpG. Dabei handelt es sich um einen bloss lesenden Zugriff, welcher auf Meldungen zum Coronavirus Sars-CoV-2 beschränkt ist. Dabei ist der Zugriff wiederum auf diejenigen Meldungen beschränkt, die zur Generierung des Freischaltcodes – d.h. zur Verifizierung eines positiven Testresultats im konkreten Fall – erforderlich ist (Art. 93 Abs. 1 Bst. a^{bis} der Epidemienverordnung vom 29. April 2015 [EpV, SR 818.101.1]).

In allen Fällen ist die Zugriffsberechtigung auf das Codeverwaltungssystem stets auf die Generierung eines Codes nach einer nachgewiesenen Infektion beschränkt; es besteht kein lesender oder bearbeitender Zugriff auf Daten des PT-Systems.

Absatz 2 schreibt vor, dass die zugriffsberechtigten Personen sich über das zentrale Zugriffs- und Berechtigungssystem der Bundesverwaltung für Webapplikationen (eIAM-System) anmelden (wofür sie eine elektronische Identität benötigen).

Gemäss *Absatz 3* erteilt und verwaltet das BAG die Zugriffsrechte. Es kann Kantonsärztinnen und Kantonsärzte, den Oberfeldarzt der Armee oder einzelne ihrer Hilfspersonen dazu berechtigen, die Zugriffsrechte an Hilfspersonen zu vergeben. Dabei ist zu beachten, dass das BAG gestützt auf Artikel 10 Absatz 2 die Vergabe der Zugriffsberechtigungen auch an Dritte übertragen kann.

Artikel 9a Zugriff auf das Codeverwaltungssystem über die Schnittstelle

Wie in den Erläuterungen zu Artikel 8a ausgeführt, kann die Generierung des Freischaltcodes nicht nur durch die zugriffsberechtigte Fachperson über ihren Zugriff auf das Frontend des Codeverwaltungssystem ausgelöst werden, sondern auch via Schnittstelle zwischen dem von der berechtigten Stelle verwendeten System und dem Codeverwaltungssystem. Dabei sind verschiedene technische Umsetzungsmöglichkeiten denkbar, ohne dass die Verordnung eine bestimmte vorschreiben würde. So kann z.B. die bearbeitende Person entweder den Auftrag zur Generierung eines Freischaltcodes in ihrem System eingeben, welches sodann über die Schnittstelle beim Codeverwaltungssystem den Freischaltcode anfordert oder dieser Schritt wird automatisiert durchgeführt, indem beispielsweise die infizierte Person vorgängig in einem Online-Formular den Freischaltcode bei positivem Testergebnis angefordert hat. Damit sichergestellt werden kann, dass der Freischaltcode auch hier mit dem richtigen Datum nach Artikel 6 Absatz 1 ausgestellt wird, muss die Fachperson vorgängig bei der Testabnahme den Zeitpunkt des Auftretens der Symptome erfragen und dies in ihrem System (und damit unter Verwendung der Schnittstelle im Codeverwaltungssystem) eintragen. Auch dieser Schritt kann jedoch automatisiert erfolgen, beispielsweise indem die getestete Person das entsprechende Datum ebenfalls bereits in einem Online-Formular eingibt, welches sodann direkt ins System der Gesundheitseinrichtung übertragen wird. Falls die getestete Person asymptomatisch ist, wird das Testdatum eingetragen.

Dabei gilt es zu beachten:

- Die Generierung der Freischaltcodes wird zwar über die Schnittstelle angefordert, jedoch trotzdem im Einzelfall und nicht auf Vorrat erstellt. Es wird vom System jeweils nur dann ein Freischaltcode angefordert, wenn es eine konkrete positiv getestete Person gibt, welche die SwissCovid-App tatsächlich nutzt.
- Das BAG prüft vor Anschluss der Schnittstelle, ob das System sicher und vor Missbrauch geschützt ist, bevor es den mit einem Zertifikat gesicherten Zugriff auf das Codeverwaltungssystem zulässt. Dabei überprüft es auch, dass die Freischaltcodes nicht im eigenen System der Gesundheitseinrichtung abgespeichert werden, da dies eine Verletzung der in Artikel 13 Absatz 2 aufgeführten Bestimmungen über die Vernichtung der Daten bedeuten würde.

Artikel 10 Leistungen Dritter

Absatz 1 erlaubt dem systembetreibenden BAG, Dritte zu beauftragen, den SwissCovid-Apps die Liste der für die Benachrichtigungen erforderlichen Daten im Abrufverfahren zur Verfügung zu stellen. Konkret nutzt das BAG (respektive in dessen Auftrag wiederum das BIT) aktuell Amazon Webservices, um die Liste mit den privaten Schlüsseln über deren Content Delivery Network (CDN) zu verteilen. Die Nutzung dieses Dienstes ist erforderlich, weil die (potenziell Millionen von) SwissCovid-Apps in einer hohen Frequenz nach Updates dieser Liste nachfragen, womit eine riesige Anzahl von Abfragen verarbeitet werden muss. Auch beauftragte Dritte können die auf der Liste erfassten anonymen privaten Schlüssel von infizierten Personen keinen Personen zuordnen.

Im Weiteren kann das BAG nach *Absatz 2* geeignete private oder öffentliche Organisationen mit der Vergabe (und damit auch der Verwaltung) der Zugriffsberechtigungen auf das Codeverwaltungssystem beauftragen. Der gegebenenfalls beauftragte Dritte muss Gewähr für eine zuverlässige und rechtlich korrekte Überprüfung der Berechtigung der Fachpersonen bieten.

Absatz 3 schreibt vor, dass dermassen beauftragte Dritte vertraglich verpflichtet sein müssen, die Vorgaben nach Artikel 60a EpG und dieser Verordnung einzuhalten. Dazu hat das BAG (respektive gegebenenfalls in dessen Auftrag das BIT) entsprechende Verträge abzuschliessen und die Einhaltung dieser Vorgaben zu kontrollieren. Die Bestimmung stellt zudem klar, dass davon die Regelung betreffend den Quellcode nach Artikel 60a Absatz 5 Buchstabe e EpG ausgenommen ist. So hat der Gesetzgeber diese Vorgabe, dass der Quellcode aller Komponenten des PT-Systems öffentlich ist, im Bewusstsein verabschiedet, dass für die Verteilung der Liste mit den privaten Schlüsseln das CDN von Amazon Webservices genutzt wird und dass insofern der Quellcode nicht öffentlich ist.

Artikel 11 Protokoll über Zugriffe

Absatz 1 regelt die anwendbaren Vorschriften für die Speicherung und Auswertung von Logdaten. So werden die Zugriffe der berechtigten Fachpersonen zur Generierung des Freischaltcodes zum Zweck der Datensicherheit geloggt. Bei der Benutzung des VA-Systems werden zudem beim Eintritt des Datenverkehrs in das Bundesnetzwerk zum Zweck der Sicherung der elektronischen Infrastruktur die Randdaten zu diesen Kommunikationsdaten geloggt. Zur Verhinderung einer personenbezogenen Auswertung bei der Datenübermittlung eines infizierten Teilnehmers oder einer infizierten Teilnehmerin wird zusätzlicher Datenverkehr generiert. Es ist den Bundesbehörden nicht möglich, eine Infizierung einer bestimmten Person, einem bestimmten Mobiltelefon oder einer bestimmten SwissCovid-App zuzuordnen. Die Speicherung und Auswertung der betreffenden Protokolle untersteht den Artikeln 57i–57q des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG; SR 172.010) und der Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442). Im Weiteren werden auch Logs der Zugriffe auf die Liste nach Artikel 10 Absatz 1 (d.h. im CDN von Amazon Webservices) erstellt. Der aktuell beauftragte Dritte Amazon Webservices ist vertraglich verpflichtet, diese in der Region «EU (Frankfurt)» zu speichern und selber nicht zu verwenden. Das BIT verfügt über einen Zugriff auf diese Logdaten. Die genannten Bestimmungen werden auch für die Speicherung und Auswertung dieser Protokolle durch das BIT für anwendbar erklärt.

Absatz 2 stellt sodann klar, dass das PT-System über diese Protokolle und die Aufzeichnung von Annäherungen hinaus keine Protokolle von Aktivitäten des Frontends des Codeverwaltungssystems und der SwissCovid-Apps aufzeichnet.

Artikel 12 Bekanntgabe zu Statistikzwecken

Das BAG stellt dem Bundesamt für Statistik (BFS) periodisch den aktuellen Stand der in den beiden Backends vorhandenen Daten für statistische Auswertungen zur Verfügung (vgl. Art. 60a Abs. 2 Satz 1 EpG). Diese Daten werden dem BFS in vollständig anonymisierter Form zur Verfügung gestellt, um rudimentäre statistische Auswertungen zu ermöglichen (insb. Anzahl der von den berechtigten Fachpersonen generierten Freischaltcodes und der von teilnehmenden Personen in der SwissCovid-App eingegebenen Freischaltcodes). Diesbezüglich gilt zu beachten, dass auch das BFS gemäss Artikel 13 Absatz 5 verpflichtet ist, diese Daten innerhalb der jeweiligen Fristen nach Artikel 13 zu vernichten. Es bleibt somit ausgeschlossen, dass zu Statistikzwecken Daten länger aufbewahrt werden dürfen, als es für die Benachrichtigung gemäss Artikel 5 Absatz 2 Buchstabe e erforderlich wäre (vgl. Art. 60a Abs. 5

Bst. d EpG).

Artikel 13 Vernichtung der Daten

Die mit dem PT-System bearbeiteten Daten sind zu vernichten, sobald sie für die Benachrichtigung der teilnehmenden Personen nicht mehr erforderlich sind (Art. 60a Abs. 5 Bst. d EpG). Dies bedingt unterschiedliche Zeitpunkte für die Vernichtung:

- *Abs. 1:* Die Annäherungsdaten, welche lediglich für den Zeitraum einer möglichen Ansteckung relevant sind, werden fortlaufend nach 14 Tagen gelöscht.
- *Abs. 2:* Der Freischaltcode wird 24 Stunden nach der Erstellung durch die medizinische Fachperson gelöscht und zwar unabhängig davon, ob er verwendet wurde oder nicht.
- *Abs. 3:* Protokolldaten von nach Artikel 10 Absatz 1 beauftragten Dritten werden 7 Tage nach ihrer Erfassung vernichtet.
- *Abs. 4:* Im Übrigen richtet sich die Vernichtung der Protokolldaten nach Artikel 4 Absatz 1 Buchstabe b der Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442).

Nach *Absatz 5* sind die dem BFS für statistische Auswertungen zur Verfügung gestellten Daten ebenfalls gemäss diesen Vorgaben zu vernichten.

Artikel 14 Überprüfung des Quellcodes

Die maschinenlesbaren Programme des PT-Systems müssen nachweislich aus dem öffentlichen Quellcode erstellt worden sein (Art. 60a Abs. 5 Bst. e EpG). Gemäss *Absatz 1* veröffentlicht das BAG die Daten, welche dazu dienen, zu überprüfen, ob die maschinenlesbaren Programme aller Komponenten des PT-Systems aus dem veröffentlichten Quellcode erstellt worden sind. Demnach wird der entsprechende Nachweis in erster Linie dadurch erbracht, dass technisch versierte Interessierte anhand der vom BAG veröffentlichten Daten grundsätzlich überprüfen können, dass die maschinenlesbaren Programme tatsächlich aus dem veröffentlichten Quellcode erstellt worden sind.

Gemäss *Absatz 2* nimmt das BAG die entsprechende Überprüfung auch selbst vor. Diese Anforderung ergibt sich für das systembetreibende BAG bereits aus der Pflicht, den Quellcode zu veröffentlichen (Art. 60a Abs. 5 Bst. e Satz 1 EpG).

In diesem Zusammenhang ist wiederum zu beachten, dass die Quellcodes jeweils nicht öffentlich sind für die über die Schnittstelle genutzten Funktionen der Betriebssysteme (Art. 5 Abs. 3) und für die beauftragten Dritten gemäss Artikel 10 Absatz 3.

Artikel 15 Deaktivierung der SwissCovid-App und Berichterstattung

Das BAG deaktiviert und deinstalliert beim Ausserkrafttreten der Verordnung respektive bei der Einstellung des Systems dessen Komponenten. Durch Ausschalten der beiden Backends werden zwar die SwissCovid-Apps deaktiviert. Das BAG kann aber die SwissCovid-Apps auf den Mobiltelefonen der teilnehmenden Personen nicht selbst deinstallieren. *Absatz 1* hält daher fest, dass das BAG zusätzlich zur Deaktivierung der Apps auch die teilnehmenden Personen auffordert, die SwissCovid-App auf dem Mobiltelefon zu deinstallieren.

Das PT-System wurde zum ersten Mal in dieser Art entwickelt und der Bund hat mit einer solchen Entwicklung Neuland betreten. Damit abgeschätzt werden kann, wie sinnvoll ein solches System ist, und im Hinblick auf allfällige vergleichbare Epidemien statuiert *Absatz 2* daher, dass das BAG dem Bundesrat spätestens sechs Monate nach dem Ausserkrafttreten der vorliegenden Verordnung Bericht erstattet.

Artikel 15a Verbindung des PT-Systems mit entsprechenden ausländischen Systemen

Das PT-System darf gemäss Artikel 62a EpG nur mit einem ausländischen System verbunden werden, wenn dieses dem PT-System entspricht und im betreffenden Staat ein angemessener Schutz der Persönlichkeit gewährleistet wird, entweder durch Gesetzgebung oder durch hinreichende Garantien, insbesondere durch Vertrag.

Absatz 1 konkretisiert die Anforderungen an ausländische Systeme, damit sie als dem PT-System «entsprechend» angesehen werden können. Ausländische Systeme gelten als entsprechend, wenn sie die Voraussetzungen an das PT-System nach Artikel 60 Absatz 5 Buchstaben a-d EpG erfüllen: Damit wird vorgeschrieben, dass nur Systeme, welche die entsprechenden Grundsätze (v.a. Privacy-by-Design, dezentrale Speicherung der Kontakte, Datensparsamkeit) einhalten, mit dem schweizerischen PT-System verbunden werden dürfen. Demgegenüber wird darauf verzichtet, die Anforderungen von Art. 60 Abs. 5 Buchstabe e EpG auf ausländische PT-Systeme zu erstrecken. Für ausländische Systeme muss daher nicht nachgewiesen werden können, dass sämtliche Komponenten auf Open-Source-Software basieren und dass die ausführbaren Programme nachweislich daraus erstellt worden sind. Würde man diese Voraussetzung auch auf ausländische Systeme erstrecken, bestünde das Risiko, dass eine Anbindung nicht möglich wäre wegen geringfügigen Weiterentwicklungen am Programmcode, die nicht Open-Source sind oder wenn der erwähnte Nachweis nicht erbracht werden kann.

Absatz 2 legt fest, dass die Verbindung über ein Verbindungssystem zur gegenseitigen Übermittlung der jeweiligen privaten Schlüssel der infizierten teilnehmenden Personen erfolgt, an welches das VA-Backend und das ausländische System angeschlossen werden.

Absatz 3 schreibt die Regeln vor, denen das Verbindungssystem untersteht:

- Gemäss *Buchstabe a* wird das Verbindungssystem entweder vom BAG oder von der zuständigen ausländischen Stelle betrieben. Das BAG bzw. die zuständige Stelle ist dafür verantwortlich, dass diese Voraussetzungen in Bezug auf zukünftige Verbindungssysteme eingehalten werden.
- Gemäss *Buchstabe b* gelten für vom BAG betriebene Verbindungssysteme dieselben Open-Source-Vorgaben wie sie für das PT-System gelten (Art. 60a Abs. 5 Bst. e EPG und Art. 14 VPTS).
- Gemäss *Buchstabe c* darf das Verbindungssystem nur im Hinblick auf die in Artikel 60a Absatz 2 EpG genannten Zwecke eingesetzt werden, d.h. zur Benachrichtigung von möglicherweise infizierten Personen. Eine polizeiliche, strafrechtliche oder nachrichtendienstliche Verwertung der Daten ist demnach ausgeschlossen.
- Gemäss *Buchstabe d* können Daten, die aus der Benutzung des Verbindungssystems resultieren, in vollständig anonymisierter Form dem BFS oder einer entsprechenden ausländischen Stelle zu Statistikzwecken übermittelt werden (vgl. Art. 60a Abs. 2 EpG).
- Gemäss *Buchstabe e* darf das Verbindungssystem Daten nur solange speichern, wie es für die Benachrichtigung der teilnehmenden Personen erforderlich ist; in jedem Fall längstens aber für 14 Tage (vgl. Art. 60a Abs. 5 Bst. d EpG; Art. 13 Abs. 1 VPTS).

Absatz 4 beschreibt die Erweiterungen der Funktionsweisen nach den Artikeln 5 und 6 für den Fall, dass das schweizerische System mit einem entsprechenden ausländischen System verbunden wird. Demgemäss werden die Schlüssel der als infiziert geltenden Personen vom ausländischen PT-System über das Verbindungssystem auf das schweizerische VA-Backend übertragen (*Bst. a*). Umgekehrt werden die privaten Schlüssel der Benutzer der SwissCovid-App im Falle einer Infektion, d.h. bei Eingabe des Freischaltcodes, über das Verbindungssystem an das entsprechende ausländische VA-Backend geliefert (*Bst. b*). Eine gesonderte Einwilligung für die Bekanntgabe der Schlüssel an ausländische PT-Systeme der teilnehmenden Personen ist weder vorausgesetzt noch vorgesehen. Dies würde die Effektivität der internationalen Interoperabilität, insbesondere hinsichtlich der grenzüberschreitenden Übertragung des Virus, entscheidend beeinträchtigen (siehe Internationale Interoperabilität, Ziff. 2 vorstehend). Ausserdem bestünden keine sachlichen Gründe für eine Ungleichbehandlung bzw. Selektion von einzelnen (ausländischen) Systemen, zumal nur entsprechende Systeme verbunden werden dürfen.

Artikel 16 Aufhebung eines anderen Erlasses

Mit der definitiven Einführung des PT-Systems wird der Pilotversuch abgeschlossen, weshalb auch die Covid-19-Verordnung Pilotversuch Proximity-Tracing hinfällig wird. Sie wird mit Inkrafttreten der vorliegenden Verordnung aufgehoben.

Artikel 16a Nachführung des Anhangs

Das EDI führt die Annäherungsbedingungen (Art. 5 Abs. 2 Bst. e) und die Anzahl abzugehender Tage (d.h. den Beginn des epidemiologisch relevanten Zeitraums nach Art. 6 Abs. 3) im Anhang entsprechend dem aktuellen Stand der Wissenschaften nach.

Artikel 17 Inkrafttreten und Geltungsdauer

Die am 19. Juni 2020 verabschiedete dringliche Änderung des EpG im Zusammenhang mit dem Coronavirus (Proximity-Tracing-System) gilt bis zum 30. Juni 2022; danach sind alle darin enthaltenen Änderungen hinfällig. Dabei ist der Bundesrat direkt gestützt auf Artikel 60a Absatz 8 EpG verpflichtet, das PT-System bereits vorher einzustellen, wenn es sich als nicht mehr notwendig oder nicht genügend wirksam erweist. Entsprechend hält Artikel 17 fest, dass die Verordnung bis längstens zum 30. Juni 2022 gilt. Dieselbe Befristung gilt ebenfalls für Artikel 93 Absatz 1 Buchstabe a^{bis} EpV.

Mit Blick auf Artikel 60a Absatz 8 EpG muss sich der Bundesrat folglich kontinuierlich vergewissern, dass der Betrieb des PT-Systems notwendig und genügend wirksam ist. Ist dies nicht mehr der Fall, muss er die Einstellung des Betriebs anordnen (durch eine Änderung oder Aufhebung der vorliegenden Verordnung). Diesbezüglich ist zu beachten, dass das systembetreibende BAG zugleich auch zuständig ist, dem EDI zuhanden des Bundesrats die dafür notwendigen Anträge zu stellen (Art. 9 Abs. 3 Bst. a Ziff. 1 der Organisationsverordnung vom 28. Juni 2000 für das EDI, SR 172.212.1).